North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Officials say package found at Fort Snelling was harmless.** Part of a federal office building at the Ft. Snelling complex in Minnesota was evacuated November 15 after an employee discovered a suspicious package containing a white powdery substance. Authorities were notified after the package was found around 9 a.m. The individual who found the package had opened it and got a small amount of the suspicious material on his hands. Firefighters quickly responded and secured a small area of the Bishop Henry Whipple Federal Building, at 1 Federal Drive in St. Paul. Employees working in that section were evacuated while hazmat specialists removed the package and its contents. As a precaution, the individual who found the package was placed under quarantine. The Bishop Henry Whipple Federal Building houses six federal agencies and about 1,900 employees. A spokesman with the U.S. General Services Administration said initial tests showed the white powder is harmless talc. Source: http://www.kare11.com/news/news_article.aspx?storyid=882485&catid=391

(Minnesota) **Slow process to remove old Minnesota dams.** Minnesota has hundreds of aging dams that are no longer needed, some in danger of failing. The dams were built in the early 1900s to run sawmills, make electricity, create lakes, and control flooding. The state Department of Natural Resources (DNR) has identified about 100 dams that need to be torn down, repaired or modified. And, the agency is working against time as it expects more dam failures like the one in Oronoco earlier this fall. Minnesota Public Radio News said the DNR receives $2 million per year to work on the dams, so only 17 have been removed and 25 have been modified to improve safety and wildlife habitat. Source: http://www.ksfy.com/Global/story.asp?S=13491178

(Montana) **Montana firefighter says he started forest fire.** A 26-year-old firefighter from Dillon, Montana, said he started a fire in the Beaverhead-Deerlodge National Forest and later worked on the Forest Service crew that extinguished the blaze. The suspect appeared in federal court in Missoula November 16 and pleaded guilty to damaging government property, a misdemeanor. Sentencing is set for January 5. Prosecutors said the suspect and a 23-year-old man, also of Dillon, lit beetle-killed trees on fire in the Birch Creek area October 18, 2009. The fire burned about one-tenth of an acre, and the firefighter suspect was involved in the suppression effort. Authorities used distinctive tire tracks left at the scene to find the 23-year-old suspect, who also pleaded guilty to damaging government property. Source: http://www.kulr8.com/news/state/108915194.html

(Wyoming) **Brucellosis confirmed in Park County.** The Wyoming State Veterinarian has been notified that cultures for Brucellosis are positive on cattle from one Park County cattle herd. Results were received November 9 from the National Veterinary Services Laboratory (NVSL) in Ames, Iowa, and the

Wyoming State Veterinary Laboratory (WSVL) in Laramie, Wyoming. Brucella abortus Biovar 1 was isolated from milk and tissue cultures from one of the cows found with a reactor titer to blood tests conducted at WSVL October 25. The U.S. Department of Agriculture's Animal and Plant Inspection Service will designate the herd from which the reactor cows originated as "Brucellosis affected" as of November 11. Three cows that originated from a herd within Wyoming's Designated Surveillance Area (DSA) were positive to blood tests at a Wyoming livestock auction market. Specified cattle from the DSA are required to be tested within 30 days prior to change of ownership or movement from counties within the DSA. The herd was quarantined October 26. Source: http://www.littlechicagoreview.com/view/bookmark/10269965/article-Brucellosis-confirmed-in-Park-County?instance=news

National

Lead taints reusable shopping bags. A number of reusable bags available at major retailers and supermarkets are tainted with lead, according to an investigation by the Tampa Tribune. The lead, contained in the paint on the outside of the bags, is not likely to rub off on foodstuffs, but the levels of the toxic metal are high enough that the bags would be considered hazardous waste by the county health department featured in the Tribune's report. A Senator from New York has called for a federal investigation into the safety of the grocery bags. Source: http://www.startribune.com/local/108521729.html?elr=KArksDyycyUtyycyUiD3aPc:_Yyc:aUokEya_tyycy_eEQDU

(Michigan) **More fake money hitting streets.** When federal agents busted a counterfeiting operation in Detroit, Michigan, recently, they did not find any sophisticated engraving tools, expensive presses, or fancy paper that mimicked the real green stuff. A woman led them to a storage locker that contained a Lexmark printer and some plain paper. Federal authorities said fake money is popping up in record amounts as simple gadgets such as all-in-one printers make it easier for even the tech-illiterate to make their own money. Nationwide, the Secret Service pulled $182 million in fake bills from circulation in 2009 — more than double the $79 million in fake loot that was discovered the year before. And about 62 percent of counterfeit bills passed around in 2009 were made on digital printers, versus less than 1 percent in 1995. Source: http://www.freep.com/article/20101106/NEWS06/11060417/1318/More-fake-money-hitting-streets

International

Greek police, protesters clash at annual march. Youths hurled rocks, flares, and smashed-up paving stones at police outside the U.S. Embassy in Athens, Greece, November 17, during a mass rally to mark the anniversary of a 1973 anti-dictatorship uprising. Riot police used tear gas and stun grenades during the brief but violent confrontation with dozens of anarchists, and chased groups that dispersed down streets near the embassy building. At least 23 people were arrested, authorities said, while 3 police officers were lightly injured and 1 protester was being treated in hospital for burns. Groups of youths continued running clashes with riot police after the end of the march, while police helicopters with searchlights circled overhead. More than 6,000 officers were on duty to monitor the annual demonstration, which was generally peaceful, with more than 20,000 people marching through central Athens. Source: http://www.ajc.com/news/nation-world/greek-police-protesters-clash-744388.html

Germany: Terrorists plan attacks this month. Germany said November 17 it had firm evidence Islamist militants were planning attacks in the next 2 weeks and ordered increased security at potential targets including train stations and airports. "The security situation in Germany has become more serious," said Germany's top security official. "We have concrete indications of a series of attacks planned for the end of November," he said. This is the first time German officials have referred to "concrete" intelligence in reference to a terrorism investigation. A series of recent events suggest authorities are dealing "with a new situation," according to the official. Source: http://www.msnbc.msn.com/id/40230005/ns/world_news-europe/

Hungary's toxic sludge reaches Ukraine. Water contaminants from a toxic discharge from an aluminum plant in Hungary have reached Ukrainian waters, scientists discovered. Scientists at the Ukrainian Scientific Center for Sea Ecology found that polluting agents from an October industrial accident reached Ukraine, the National News Agency of Ukraine reports. Toxic sludge reached a tributary of the Danube River after leaking from a chemical plant about 100 miles west of Budapest. The plant held toxic byproducts left from the conversion of bauxite to aluminum. Around 24 million cubic feet of toxic red mud covered Hungarian buildings in October, leaving at least seven people dead and injuring more than 120 others. The Hungarian government declared a state of emergency in three counties close to the spill, and authorities suspended work at the aluminum plant. Ukrainian environmentalists reported that the level of contamination in area waters was considered high, but not critical enough to warrant an extreme threat to public health. Source: http://www.upi.com/Science_News/Resource-Wars/2010/11/12/Hungarys-toxic-sludge-reaches-Ukraine/UPI-65911289561914/

Canada scans mails for bombs. Canadian border agents are inspecting courier packages entering the country they suspect might contain explosives. The heightened security follows the discovery of two printer toner cartridge bombs on flights bound for the United States late last October. British police said November 10 one of the bombs seized October 29 was set to detonate over Canadian airspace. Niagara Regional Police and the Canada Border Services Agency were called November 10 to a courier facility at the busy Niagara Falls, Ontario, border crossing that serves as an clearing house for packages entering the country from the United States. Officers were required to conduct "a sweep" for possible explosives after workers reported a suspicious package, police said. But none were found. "Everyone is on a heightened state of alert," one worker at a courier firm said. "There were officers scrambling to the depot." Source: http://www.sherwoodparknews.com/ArticleDisplay.aspx?e=2843493

Mexico violence costs $350K daily in natural gas losses. Threats and violence by drug gangs are preventing some government oil workers from reaching installations in northern Mexico and costing state-owned Petroleos Mexicanos (Pemex) about $350,000 every day in lost production, a company official said November 11. The official said Pemex has shut down the equivalent of about 100 million cubic feet of natural gas production per day. That amounts to about $10.5 million per month, or about 2.3 percent of Mexico's $450 million per month average in monthly natural gas revenues. The lost production is centered in the Burgos gas field near the east Texas border in an area where drug gangs have threatened and kidnapped Pemex workers at some of the company's installations. The official said that earlier in the year, when the security problems were most acute, gas production was down twice as much — about 200 million cubic feet per day. The problem came to a head in May

2010, when five workers at a gas compression plant were abducted by armed men. The father of one of the victims has said the workers were warned to stay away, and the kidnapped men have not been heard from since. However, army troops are now helping Pemex provide increased security. "This has allowed us to start partially recovering the production we had stopped for this reason," the Pemex exploration and production division chief told local media. Source: http://www.theeagle.com/world/Mexico-violence-costs--350K-daily-in-natural-gas-losses

Banking and Finance Industry

European banks see new ATM skimming attacks. Banks in Europe are seeing innovative skimming attacks against ATMs, where fraudsters rig special devices to the cash machines to record payment card details. Many banks have fitted ATMs with devices that are designed to thwart criminals from attaching skimmers to the machines. But it now appears in some areas that those devices are being successfully removed and then modified for skimming, according to the latest report from the European ATM Security Team (EAST), which collects data on ATM fraud throughout Europe. Skimming devices are designed to record the account details from the magnetic stripe on the back of a payment card. The data can then be encoded onto a dummy card. A person's PIN (personal identification number) is often captured with a micro-camera, which was done with the illicitly modified anti-skimming devices, according to the report. Banks in five countries also reported seeing a new type of skimming device, which uses a modified MP3 player to record card details. It also has a micro-camera to record PINs, according to a photo seen by IDG News Service. Source: http://www.computerworld.com/s/article/9197138/European_banks_see_new_ATM_skimming_attacks

Cyber crime reaches milestone. Complaints about Internet crimes have reached a milestone. On November 9, the Internet Crime Complaint Center (IC3) logged its 2 millionth consumer complaint alleging online criminal activity. The IC3, a partnership between the FBI and the National White Collar Crime Center, became operational in May 2000 and received its 1 millionth complaint 7 years later, on June 11, 2007. It took half that time to receive the 2 millionth complaint., which may be due to the IC3's increased visibility as well as the continued growth of cyber crime. The IC3 refers cyber crime complaints to law enforcement agencies. Since its inception, the IC3 has referred 757,016 criminal complaints to law enforcement around the globe. The majority of referrals involved fraud in which the complainant incurred a financial loss. The total reported loss from these referrals is approximately $1.7 billion, with a median reported loss of more than $500 per complaint. Many complaints involved identity theft, such as loss of personally identifying data, and the unauthorized use of credit cards or bank accounts. Source: http://www.insurancejournal.com/news/national/2010/11/16/114909.htm

Chemical and Hazardous Materials Sector

(Connecticut) **Unspecified security issue found, corrected the same day at Millstone.** Federal Nuclear Regulatory Commission (NRC) inspectors discovered a security issue at the Millstone nuclear power station in Waterford, Connecticut that was preliminarily determined to be of "greater than very low" security significance during a September 28 inspection. NRC officials declined to specify the issue or define its significance, but said the problems were "corrected or compensated for" before inspectors left that day, according to a letter sent November 9 to the president and chief nuclear

officer at Dominion Resources. "The finding is also an apparent violation of NRC requirements and is therefore being considered for escalated enforcement action in accordance with the NRC's Enforcement Policy," stated the letter, signed by the NRC director of reactor safety. Although the letter was made public, the inspectors' report defining the problems will remain confidential. Dominion has 30 days to respond. Source: http://www.theday.com/article/20101111/NWS01/311119398/1044

Commercial Facilities

(Florida) **Apparent suicide by cyanide leads to hotel evacuation.** About 75 people were evacuated from a hotel in Temple Terrace, Florida, after a guest apparently committed suicide and left a note saying she took cyanide November 15, police said. The Extended Stay America Hotel remained vacant November 16 as owners waited for an independent contractor to sanitize the building. The investigation began when Temple Terrace police received a call that a woman in her hotel room was suffering from cardiac arrest. When officers went to her room to investigate, they found a note that said she had consumed cyanide. Police also found a powdery substance in her room but do not know what it is, a police spokesman said. Along with examining rooms and hallways, officials are also examining officers, paramedics, and firefighters who were in the room and general vicinity and had contact with the victim, he said. Source: http://www2.tbo.com/content/2010/nov/15/160639/temple-terrace-hotel-evacuated-after-woman-claimed/news-breaking/

Communications Sector

Emergency broadcast system coming to cell phones. The communications company Alcatel-Lucent announced November 16 that it is creating a Broadcast Message Center that will allow government agencies to send cell phone users specific information in the event of a local, state, or national emergency. It will be similar to the TV alerts in that the text messages will be geographically targeted for areas where a tornado alert or major road closure, for example, is in effect. The Broadcast Message Center is designed to help mobile phone companies comply with new federal rules outlined in the Federal Communication Commission's (FCC) Commercial Mobile Alert System, the Urgent Communications journal reported. Under the new system, all phones would receive emergency alerts directly from the U.S. government about terrorist attacks or natural disasters, but users can opt out of receiving local warnings about weather, traffic accidents, or Amber Alerts. The system has already been tested in California and Florida, and is expected to be up and running in compliance with FCC guidelines by April 2012. Source: http://www.aolnews.com/nation/article/emergency-broadcast-system-coming-to-cell-phones/19721588

U.S. Department of Commerce takes major step towards unleashing the wireless broadband revolution. The Commerce Department, through the National Telecommunications and Information Administration (NTIA), announced November 16 that it is recommending that 115 MHz of spectrum be reallocated for wireless broadband service within the next 5 years — an important step towards achieving the President's goal to nearly double the amount of commercial spectrum available over the next decade. NTIA released two complementary reports detailing the effort to nearly double commercial wireless spectrum: a Ten-Year Plan and Timetable, as well as a Fast Track Evaluation identifying the 115 megahertz of spectrum to be made available within 5 years. NTIA developed the

Ten-Year Plan and Timetable in response to the June 28, 2010 Presidential Memorandum that directed the Secretary of Commerce, working through NTIA, to collaborate with the Federal Communications Commission (FCC) to make available a total of 500 megahertz of federal and nonfederal spectrum over the next 10 years for mobile and fixed wireless broadband use. The report, developed with input from other Federal agencies and the FCC, identifies 2,200 megahertz of spectrum for evaluation, the process for evaluating these candidate bands, and the steps necessary to make the selected spectrum available for wireless broadband services. Source: http://m2m.tmcnet.com/news/2010/11/16/5139929.htm

T-Mobile Samsung Galaxy Tab hacked to enable voice calls. Not long after the launch of the Samsung Galaxy Tab for T-Mobile, the enterprising hackers of XDA-Developers have developed a method to re-enable voice calling via the device, although the method is more involved for the average modder. The U.S. version of the Galaxy Tab has had its voice calling capability removed by Samsung, whereas the European carrier and unlocked versions tout voice calling over Bluetooth or the built-in microphone as a feature. Source: http://www.phonenews.com/t-mobile-samsung-galaxy-tab-hacked-to-enable-voice-calls-13816/

Smartphones in hacking risk. Certain smartphone models running Google's Android operating system have security flaws that could allow hackers to steal personal information or record conversations, researchers said. In a demonstration at a Black Hat security conference, a UK researcher showed how a vulnerability in the Web browser on an HTC Android phone allowed him to install an application that gave him broad control over the phone. Another method of attack is to get a user to install a seemingly harmless application, which can then be used to access data. The researcher from MWR InfoSecurity showed the application could re-install itself with greater privileges and give a hacker broad powers, including recording. The Black Hat presentation was the latest in a series of findings in the past 1 weeks raising concerns about the security of Android phones, which have overtaken those made by Apple to claim 25 percent of the global market in the third quarter. Another team presented a similar scenario at a security conference in Oregon, using what appeared to be an innocuous application for a popular game — Angry Birds — that in turn installed malicious programs. "We've begun rolling out a fix for this issue, which will apply to all Android devices," Google said. While there have been few reports of criminals using such techniques yet, experts said it was only a matter of time. Source: http://www.ft.com/cms/s/2/c56d7a58-edc1-11df-9612-00144feab49a.html#axzz154dCX3G5

Google's Street View cars may have violated federal laws. Just weeks after the Federal Trade Commission dropped its inquiry, the Federal Communications Commission (FCC) is confirming its own investigation of Google's inadvertent collection of private information. In October 2010, Google announced it had accidentally picked up and recorded e-mails, passwords, and other personal information when its Street View cars used Wi-Fi networks and GPS data to capture street-level images for Google Maps. "In light of their public disclosure, we can now confirm that the enforcement bureau is looking into whether these actions violate the communications act," the chief of the FCC's enforcement bureau, said in a statement. "As the agency charged with overseeing the public airwaves, we are committed to ensuring that the consumers affected by this breach of privacy receive a full and fair accounting." The investigation dates back to May 2010, when the FCC received a complaint from the Electronic Privacy Information Center (EPIC), an advocacy group that focuses on emerging civil liberties and privacy issues. EPIC wanted the FCC to determine whether Google was

violating federal electronic eavesdropping laws. Besides the FCC probe, several European countries launched their own investigations about possible privacy breaches from Street View. Source: http://www.neontommy.com/news/2010/11/googles-street-view-cars-may-have-violated-federal-laws

CRITICAL MANUFACTURING

Qantas: 40 engines on A380s need to be replaced. As many as half of the 80 Rolls-Royce engines that power some of the world's largest jetliners may have to be replaced after an oil leak caused a fire and the partial disintegration of one on a Qantas flight in November, the Australian national airline's chief executive said November 18. The 40 potentially faulty engines on the Airbus A380 would need to be replaced with new engines while the fault is fixed, raising the specter of engine shortages that could delay future deliveries of the 7-story-tall superjumbo. It was not clear how serious the problem would be, but the comments by Qantas's CEO were the most definite accounting yet of a problem that now appears larger than first imagined when one of his airline's engines came apart over Indonesia, spewing metal shrapnel into a wing and severing vital operating systems. Qantas has grounded its fleet of six A380s, each powered by four of the giant Rolls-Royce Trent 900 engine. Qantas's CEO told reporters that Qantas may have to replace 14 engines, each worth about $10 million. Source: http://www.huffingtonpost.com/huff-wires/20101118/superjumbo-woes/

Rolls-Royce confirms faulty part caused Qantas flight explosion. Rolls-Royce confirmed November 12 a faulty engine part was behind an explosion that forced A380 Qantas flight QF32 to make an emergency landing in Texas the week of November 1. â¨â¨The failure of a specific component in the turbine area of the engine started an oil fire, which caused the engine to explode mid-air. â¨â¨The aerospace manufacturer would not confirm the nature of the component, the supplier of the part, or whether it could be obtained elsewhere. â¨â¨A Rolls-Royce spokesman said the fault only related to its Trent 900 engine types. It currently supplies these engines to three major airlines - Qantas, Lufthansa, and Singapore Airlines. The European Aviation Safety Agency issued an emergency directive November 11 demanding regular checks on all Trent 900 engines made by Rolls-Royce. Source: http://www.supplymanagement.com/news/2010/rolls-royce-confirms-faulty-part-caused-qantas-flight-explosion/

Recall: Nissan, GM, and Chrysler vehicles. Nissan announced a recall November 11 to replace the lower steering column joint and shaft on 303,000 2002-2004 Frontier and 283,000 2002-2004 Xterra vehicles, and the positive battery cable terminal on 18,500 2010-2011 Sentra vehicles in several markets in North and South America and Africa. No accidents or injuries have been reported with either issue. Nissan found that in certain rare instances, the lower steering column joint on the affected Frontier and Xterra vehicles can develop corrosion that limits movement. If the vehicle continues to be driven in this condition it may, in an extreme case, lead to cracking of the steering shaft. On some affected Sentra vehicles, an issue with the connector on the positive battery cable terminal could lead to difficulty starting the vehicle, and in rare cases, a possibility of stalling at low speeds. The potentially affected Frontier and Xterra vehicles were manufactured in Tennessee, between July 2001 and January 2005, and in Brazil between November 2001 and June 2008. The potentially affected Sentra vehicles were manufactured in Mexico between May 22, 2010 and July 8, 2010. Nissan plans to begin owner notification in early December once replacement parts are available. Additionally, GM recalled 14,245 Cadillac DTS and V8 Buick Lucerne Models November 11

from the 2010 and 2011 model year for a power steering issue that has resulted in fires in four vehicles. Chrysler, meanwhile, is recalling about 16,000 Jeep Liberty SUVs from the 2008 model year to fix faulty windshield wiper systems. Source: http://blogs.consumerreports.org/cars/2010/11/nissan-gm-chrysler-recalls-frontier-xterra-and-sentra-vehicles.html

Defense/ Industry Base Sector

Lockheed finds cracks in F-35B test aircraft. Lockheed Martin has discovered a potentially significant problem with one model of its F-35 joint strike fighter, the company reported November 17. Lockheed issued a statement saying its Fort Worth engineering staff had found cracks in the rear bulkhead — a major structural part weighing about 300 pounds — of an F-35B ground test plane undergoing fatigue testing. The cracks were found after the plane had been subjected to the equivalent of about 1,500 hours of flight time. The airplane's structural components are designed to last at least 8,000 hours. Lockheed said the cracks were found in a special inspection after engineers discovered unusual data from test instruments. The latest problem comes at a key juncture for the troubled F-35, which, at an estimated $382 billion, is the costliest weapons program ever. Source: http://www.star-telegram.com/2010/11/17/2640453/lockheed-finds-cracks-in-f-35b.html

U.S. Navy amphibs 'combat ineffective': Pentagon report. A recently leaked Pentagon evaluation called the U.S. Navy's San Antonio-class amphibious transport dock ships used to transport U.S. Marines and position them for beach landings "combat ineffective." The Navy, however, said the process to correct the ships' shortcomings is already well underway, and officials insist the ships are "warfare capable." Five of the ships have been commissioned. Four ships are under construction; a total of 11 ships are planned. The ship is manufactured by Northrup-Grumman. Source: http://www.defensenews.com/story.php?i=5046685&c=SEA&s=TOP

Emergency Services

F.B.I. seeks wider wiretap law for web. The director of the FBI traveled to Silicon Valley in California November 16 to meet with top executives of several technology firms about a proposal to make it easier to wiretap Internet users. The FBI director and the FBI's general counsel were scheduled to meet with senior managers of many major companies, including Google and Facebook, according to several people familiar with the discussions. The director wants to expand a 1994 law, the Communications Assistance for Law Enforcement Act, to impose regulations on Internet companies. The law requires phone and broadband network access providers to make sure they can immediately comply when presented with a court wiretapping order. Law enforcement officials want the 1994 law to also cover Internet companies because people increasingly communicate online. An interagency task force of Presidential Administration officials is trying to develop legislation and submit it to Congress early next year. Under the proposal, firms would have to design systems to intercept and unscramble encrypted messages. Services based overseas would have to route communications through a server on United States soil where they could be wiretapped. Source: http://www.nytimes.com/2010/11/17/technology/17wiretap.html?_r=1&partner=rss&emc=rss

(New York) **NYPD begins using iris scans on suspects.** Along with fingerprints and mug shots, the New York City Police Department (NYPD) is now taking photographs of the irises of crime suspects. The

NYPD said November 15 that the images will be used to help avoid cases of mistaken identity. The process takes about 5minutes. Every suspect will be scanned again using a handheld device shortly before they are arraigned to make sure the irises match. Police said the software, handheld device, and cameras cost about $23,800 each, and 21 systems will be used around the city. Central booking in Manhattan started taking photos November 15. Source: http://www.nationalterroralert.com/2010/11/15/nypd-begins-using-iris-scans-on-suspects/

Program to curb gun smuggling to Mexico found weak. There are "significant weaknesses" in a U.S. program to stem the flow of guns illegally sent to Mexico, undermining the effectiveness of the crackdown, according to the Justice Department's inspector general. The Bureau of Alcohol, Tobacco, Firearms and Explosives does not consistently exchange firearms trafficking intelligence with Mexican and U.S. partner agencies as part of its Project Gunrunner program, according to the November 9 report. It said the agency has not provided Mexican law enforcement with information it requested on firearms trafficking routes and distribution points. Project Gunrunner, part of an effort to reduce violence associated with drugs and guns on the U.S.-Mexico border, expanded from a pilot program in 2006. "Despite the increased ATF activity associated with Project Gunrunner, we found that significant weaknesses in ATF's implementation of Project Gunrunner undermine its effectiveness," according to the report. Although requests from Mexico for ATF to trace guns have increased, most requests are "unsuccessful" because of missing or improperly entered gun data, the report said. Source: http://www.businessweek.com/news/2010-11-09/program-to-curb-gun-smuggling-to-mexico-found-weak.html

More data in criminal justice cases calls for upgrade to MPLS. An expansion of exchanged data used by state, local, and federal agencies under the National Law Enforcement Telecommunications System (NLETS) is calling for a faster and cheaper means of transmitting information. Therefore, NLETS is planning to upgrade its current T1 relay service to Multiprotocol Label Switching (MPLS). Today, NLETS services expand upon providing to the FBI a typical background check using a driver's license and vehicle registration. An additional amount of shared criminal justice data among the 50 U.S. states, the federal government and several foreign countries, is outpacing available bandwidth and slowing down security measures. Implementing MPLS will let NLETS provide full T1 speeds to its users for about the same price as an existing 128 kilobits/sec line. Though 100 Cisco 1700 Series routers will have to be replaced, the new network will allow for member-to-member connections without utilizing the NLETS network operations in Phoenix, Arizona. The new routers will also provide a backup system through the use of cellular network cards. Source: http://mpls.tmcnet.com/topics/mpls/articles/116420-more-data-criminal-justice-cases-calls-upgrade-mpls.htm

ENERGY

MSHA: Increase amount of rock dust to decrease chances of underground explosions. Starting November 22, the Mine Safety and Health Administration (MSHA) is requiring underground coal mines to increase the amount of rock dust. Officials said a study proves this will help decrease the chances of explosions. MSHA officials held a public hearing in Lexington, Kentucky to discuss whether to make the rule permanent. MSHA officials said underground coal miners could be at risk under current standards for rock dust. A recent National Institute for Occupational Safety and Health study shows the 65 percent rock dust standard is not enough to prevent an explosion. MSHA is now

requiring underground coal mines to increase incombustible rock dust to 80 percent. Researchers said the current 65 percent was set in the 1920s, but now mining methods and equipment have changed and the rock dust standards need to change too. MSHA used a study on explosions that happened in 1976 to 2001 and believe this 80 percent standard could have made a difference in six explosions that killed 46 people. The change could cost more than $22 million to implement. The final decision on the rule will come in June 2011. Source: http://www.wkyt.com/wymtnews/headlines/MSHA__108580394.html

(Washington) **Thousands still without power after powerful storm batters region.** Thousands of people were still in the dark November 16, hours after heavy winds battered Western Washington. November 15's storm brought wind gusts as high as 60 mph in some places, cutting power to more than 150,000 customers across the region. Several school districts were forced to cancel or delay the start of classes because their buildings were still without power. By 7:30 a.m., Seattle City Light said it had about 1,300 customers still without power and hoped to have all service restored by noon. Tacoma Power reported 20,000 still without power and expected all customers to be back online November 16. Snohomish PUD said 7,500 customers without power were scattered throughout the county, and 19 line crews were out working to restore service. About 76,000 Puget Sound Energy customers are still without power, and the utility said it may be November 18 before all customers have power again. Source: http://www.komonews.com/news/local/108423689.html

Food and Agriculture

Alcoholic energy drink warning issued. The Food and Drug Administration (FDA) cracked down November 17 on four manufacturers of caffeinated alcoholic drinks, giving them 15 days to stop adding caffeine to the products or stop selling them altogether. The FDA commissioner said the drinks appeared to pose a serious public health threat because the caffeine masked the effects of the alcohol, leading to "a state of wide-awake drunk." After a yearlong review found no conclusive evidence that the drinks were safe, she said, the FDA decided the caffeine in them was an illegal additive. In warning letters to the four companies — including Phusion Projects, which makes the top-selling caffeinated alcoholic drink, Four Loko — the FDA said drinking the beverages could lead to "hazardous and life-threatening situations." The letters also warned the FDA could move more aggressively, seizing the beverages from store shelves and asking a judge to halt further sales, if the companies did not take corrective action. Source: http://www.nytimes.com/2010/11/18/us/18drinks.html?_r=1&partner=rss&emc=rss

(Maine) **Oyster disease worries industry.** Oysters growers and Maine officials met recently to deal with the spread of a disease that is lethal to oysters which, while harmless to humans, could have an effect on the oyster market. Officials with the Maine Department of Marine Resources (DMR), and many of the state's oyster farmers and other experts gathered at the University of Maine's Darling Marine Center on the shore of the Damariscotta River. The purpose of the meeting was to agree on some sort of action plan in the face of an outbreak of MSX in shellfish grown in the river. According to DMR, about 70 to 75 percent of the state's $1.2 million-plus annual farmed oyster harvest comes from the Damariscotta. Neither DMR nor Maine oyster farmers have much firsthand experience with MSX – a disease caused by the parasite Haplosporidium nelsoni. But the potential for damage if the disease spreads is well documented. Mortality among oysters attacked by the disease can reach 80 to 90 percent. Several years ago, MSX nearly wiped out the oyster population of Chesapeake Bay off the

coast of Maryland and Virginia. Source: http://fenceviewer.com/site/index.php?option=com_content&view=article&id=52422:oyster-disease-worries-industry&catid=39:maritime&Itemid=65]

Feed likely source of Salmonella contamination on pig farms. Commercial feed appears to be a source of Salmonella contamination in commercial swine production units, according to a paper in the November 2010 issue of the journal Applied and Environmental Microbiology. Moreover, nearly half of isolates found in pigs were multidrug resistant. The findings suggest that pork could be a source of human infection. They also strongly question the conventional wisdom that processed feed is not a source of contamination. Heat treatment during processing has been thought to kill any bacterial contaminants. The research team, led by a researcher from the College of Veterinary Medicine at Ohio State University, tested samples collected from feed bins prior to exposure to the barn environment, as well as fecal samples and environmental samples from the barns. They found contaminated feed in eight of 36 barns tested, with a sample prevalence of 3.6 percent. These isolates fell into five different genotypes. In four of the five cases, they found that fecal samples they tested from a given barn and time point matched the feed samples from the same barn and time period, suggesting that the feed was indeed the contamination source. Source: http://www.sciencedaily.com/releases/2010/11/101116162652.htm

U.S. animal disease lab carries risks, report says. A high-security laboratory that the U.S. government wants to build in Kansas to study dangerous animal diseases could jeopardize the safety of U.S. livestock and expose them to highly contagious pathogens, according to a report requested by Congress. The proposed lab would be the world's third Biosafety-Level 4 Pathogen laboratory that could work with large animals. The other facilities are in Australia and Canada. The government wants to build the National Bio and Agro-Defense Facility (NBAF) in Manhattan, Kansas. The laboratory is part of the U.S. government's efforts to prevent natural disease outbreaks or terrorist bio-attacks on the U.S. food supply and agricultural economy. But the council's report, requested by Congress before it funds construction of the facility, said that a risk assessment conducted by DHS revealed "several major shortcomings." Among the risks, the council said, is a nearly 70 percent chance over the 50-year lifetime of the facility that the highly contagious foot-and-mouth disease (FMD) could be released, and it estimated that a spreading infection could cost the economy $9 billion to $50 billion. Source: http://www.msnbc.msn.com/id/40199157/ns/business/

NOAA opens more Gulf waters to fishing after BP spill. U.S. federal waters in the Gulf of Mexico are now almost completely open for fishing in one of the most promising signs of environmental recovery in the wake of the massive BP oil spill. The National Oceanic and Atmospheric Administration (NOAA) said November 15 it had reopened more than 8,400 square miles of Gulf waters to recreational and commercial fishermen, leaving only a fraction of the area still closed because of the spill. It was the 11th such opening since July 22. NOAA said 99.6 percent of federal waters in the Gulf were now open to fishing. Only an area covering 1,041 square miles immediately around the ruptured Macondo wellhead remains closed. Over 88,000 square miles of the Gulf were closed to fishing at one point because of the spill, stoking anger in local communities which rely heavily on the sea as a source of income and recreation. Source: http://www.reuters.com/article/idUSTRE6AE3RT20101115

Corps outlines study to keep Asian carp, other invasives from moving between watersheds. The U.S. Army Corps of Engineers released a plan November 9 to study how to prevent invasive species —

including the voracious Asian carp — from migrating between the Great Lakes and Mississippi River watersheds, calling it a "massive and complex" effort that could take years. The primary focus of the $25 million study will be on Chicago, Illinois-area waterways, where canals provide the only direct connection between the two basins. But the Corps also will look at other areas where flooding could allow invasive species to slip from one watershed to the other. Concern that the Asian carp, which can grow to 4 feet and 100 pounds, were close to Lake Michigan prompted the study. But the commander of the Corps' Great Lakes and Ohio River Division said it will look at many different types of invasive species. A final recommendation on how to stop the movement of such species — possibly by separating the watersheds permanently — is expected to be made in 2015, he said. Source: http://www.latimes.com/business/nationworld/wire/sns-ap-il-asian-carp-great-lakes,0,4684472.story

Chocolate shortage forecast. Experts believe there will be a chocolate shortage in 2010. Most of the world's cocoa crops are in West Africa. That area is suffering from a drought and crops are being destroyed by two mysterious diseases that have scientists baffled. The U.S. Department of Agriculture is working on mapping the cocoa trees' DNA to help find a cure. Forecasters predict the shortage will cause prices to shoot through the roof. Speculators said in 20 years, the average person will not be able to afford the price to satisfy their chocolate cravings. Source: http://www.39online.com/news/local/kiah-houston-chocolateshortage-story,0,3317613.story

Government Sector (including Schools and Universities)

(Illinois) **Bomb squad called out to Downers Grove police station.** Much of the Village Hall campus in Downers Grove, Illinois, was closed November 17 as the DuPage County Sheriff's Department Bomb Squad evaluated several explosive devices brought in to the Downers Grove Police Department earlier in the day. A resident who owns an estate-sale business had been preparing for a sale when she discovered a bucket of pipe bombs and other manufactured and homemade explosive devices in the home, said the Downer's Grove deputy chief. She then drove the devices to the Downers Grove station, arriving at about 5:05 p.m., he said. An officer accompanied the woman to her vehicle parked outside the police department at 825 Burlington Ave. She handed him the bucket, which he immediately set down. The bomb squad was notified and arrived on the scene at about 6:30 p.m. The deputy chief said the woman had taken a risk by transporting the explosive devices. The squad arrived in a truck that is outfitted to detonate explosives, if necessary. Source: http://downersgrove.patch.com/articles/bomb-squad-on-the-scene-at-village-hall-complex

(North Carolina) **'Numerous' bomb threats force evacuations at Bragg.** Fort Bragg officials said "numerous" bomb threats at the sprawling Army post in North Carolina have forced evacuations. A spokesman said phone threats came in to units around 12:30 p.m. November 17. First responders searched the buildings and nothing threatening was found. The buildings were reopened to personnel by late afternoon. Officials said numerous phone calls around the post include someone speaking in an unknown foreign language and saying "bomb" in broken English. The post is taking additional security measures to ensure the safety of personnel and facilities. FBI and ATF agents are on scene working with the military's criminal investigators. About 45,000 people live at Fort Bragg. Source: http://www.wral.com/news/state/story/8642545/

(Rhode Island) **Suspicious package empties federal building.** A suspicious package resulted in the evacuation of the Federal Building on Westminster Street in Providence, Rhode Island, just after noon November 17. Westminster was closed from Snow to Empire streets, and hundreds of workers and people who were doing business in the building waited from a safe distance as the state bomb squad responded to X-ray the package. The deputy fire chief said the bomb squad was called as a precaution. The package was found to be harmless. At 12:50 p.m., the building was reopened and occupants were allowed to re-enter. Source: http://newsblog.projo.com/2010/11/suspicious-package-empties-fed-1.html

Explosives found near US embassy. A fragmentation grenade and grenade launcher were found near the United States Embassy in Manila, Philippines, November 17. In a statement, a U.S. Embassy spokesperson said a street sweeper "found a bag containing possible explosive devices on the median between the Service Road and Roxas Boulevard in the vicinity of the U.S. Embassy property." The street sweeper immediately alerted an embassy guard, who in turn informed local police authorities. The incident comes at a time when the government is trying to sway other nations, including the United States, from taking back their travel advisories against the Philippines. Source: http://www.abs-cbnnews.com/nation/metro-manila/11/17/10/explosives-found-near-us-embassy

(Texas) **Feds investigate bomb threat at Austin-area school.** Texas and federal authorities are investigating a bomb threat at an Austin-area middle school a day after the threat was first made. A Williamson County sheriff's sergeant said the middle school and a nearby elementary school were evacuated about noon November 16 because of elevated concern over a call that came in late November 15. No explosives had been found on campus. Investigators called in the FBI, the Bureau of Alcohol Tobacco, Firearms, and Explosives, and the Texas Department of Public Safety. More than 1,500 students are enrolled in the two schools. Source: http://www.ketknbc.com/round-rock/feds-investigate-bomb-threat-at-austin-area-school

(Ohio) **Ohio State closes library, 3 labs in bomb scare.** Ohio State University in Columbus evacuated four buildings, including the main library, November 16 because of bomb threats e-mailed to the FBI. An FBI spokesman in Cincinnati said a threat was sent to the bureau's Washington D.C. headquarters. Campus police said they were alerted at 8:19 a.m. that the threats involved the William Oxley Thompson Memorial Library, and three laboratory buildings. All were evacuated and closed, and authorities also closed off three streets, while several helicopters circled overhead. Students and faculty were warned by text-message alerts and online and phone messages to stay clear of the area. The Columbus Fire Department bomb squad, school security, and FBI responded. Classes at the university's other academic buildings were held as scheduled. Ohio State is among the nation's largest universities with more than 56,000 students enrolled on its Columbus campus. Source: http://www.google.com/hostednews/ap/article/ALeqM5g-P5WWG3V0zEZBTi5kgDzeLWxpMA?docId=3245feb0b6614eab912022aeacd94883

Majority of government personnel do not receive enough software security training. Nearly 80 percent of personnel at government agencies and contractors said their organizations did not provide sufficient training and guidance for software security application development and delivery, according to a survey by non-profit IT security trade group (ISC) squared. Around 37 percent of those surveyed believe the first priority for improving security across the software delivery lifecycle is training and education, and 33 percent believe it should be a top priority to address culture,

attitudes, and mindsets about software security. "When the majority of information security professionals who have at least some oversight over the software development lifecycle are seeking more training and guidance, managers need to take heed," the executive director of (ISC) squared said. "In light of the industry's dependence on Web applications and its rapid migration to virtual and mobile environments, senior management must gain awareness of the grave risks involved with insecure software and create a culture that inspires education for all those involved in the software development lifecycle." Source: http://www.infosecurity-us.com/view/13916/majority-of-government-personnel-do-not-receive-enough-software-security-training/

(Illinois) **FBI joins investigation into WIU bomb threats.** FBI agents continued work with police November 11 at Western Illinois University (WIU) in Macomb, Illinois conducting interviews, following leads, and issuing additional search warrants in connection with the rash of bomb threats in the past 2 weeks on the campus. The WIU Office of Public Safety director said the FBI has provided additional resources in the investigation. Illinois State Police investigators are also working with the public safety director's office on investigating the threats and leads. Source: http://www.pjstar.com/news/x1071730482/FBI-joins-investigation-into-WIU-bomb-threats

Information Technology and Telecommunications

Senators mull bill to require private sector reporting of cyberattacks. U.S. Senators are contemplating legislation to mandate the private sector report cyberattacks in the wake of Stuxnet, a recently detected computer worm with potential to bring down industrial operations ranging from water treatment to manufacturing. At a Senate Homeland Security and Governmental Affairs Committee hearing November 17, the Chairman and Independent Senator from Connecticut, asked representatives from DHS, the computer security community and industry whether DHS needs enhanced powers to respond to threats to private networks. The Connecticut Senator and the ranking Republican Senator from Maine have sponsored the 2010 Protecting Cyberspace as a National Asset Act (S. 3480), which focuses on public-private partnerships and information sharing because industry owns upwards of 85 percent of the nation's critical infrastructure. The committee is negotiating with other Senate panels to pass comprehensive cyber legislation. The equipment vulnerable to such cyberattacks in the United States includes agricultural systems and electric grids, but the manufacturing sector is the largest user of the networks, according to DHS. Homeland Security officials who analyze and coordinate responses to incidents and threats affecting industrial control systems step in only when asked to by the private sector, said the acting director of the DHS National Cybersecurity and Communications Integration Center. He said DHS is not appealing for more powers at this time, but would not oppose accepting greater responsibilities. Source: http://www.nextgov.com/nextgov/ng_20101117_5600.php

Possible new threat: Malware that targets hardware. French researchers said it is possible to write malware that attacks specific hardware processors rather than operating systems or applications. Researchers of Ecole Supyrieure d'Informatique Electronique Automatique (ESIEA) in Paris, have developed a proof-of-concept for hardware-specific malware, which they consider a step up from Stuxnet and a potentially key weapon in cyberwarfare. The malware can easily identify and target specific hardware systems based on the on-board processor chip, the researchers said. They used the so-called floating point arithmetic (FPA) to help identify processors, including AMD, Intel Dual-Core and Atom, SPARC, Digital Alpha, Cell, and Atom. In order to pinpoint the type of processor, the

malware would see how a processor handles certain mathematical calculations. This breed of malware is not any more difficult to create than malware that targets software vulnerabilities, one researcher said. The researchers maintain that targeted attacks like Stuxnet are a major threat, but it is not always so simple for the attacker to be sure what software is running on a targeted machine. Hardware malware gives cyberwarfare another weapon. "You can arrange things in such a way that effectively Iran buys a set of computers with Intel processor of a given type and family. Then you can strike them selectively — and only these computers — whatever Iran has installed on those computers, [whether it's] Linux, Windows, or any application," he said. Source: http://www.darkreading.com/vulnerability_management/security/vulnerabilities/showArticle.jhtml;jsessionid=53HQMZG3CYRYFQE1GHPCKH4ATMY32JVN?articleID=228300082

Almost half of all rogue anti-virus was created in 2010, as UK-based spam increases. Statistics released the week of November 15 show one in ten spam messages originated from the UK. According to Trend Micro, the UK ranks top amongst western European countries for sending malicious spam, with a quarter of all scams detected created by cyber criminals in October. The most prevalent was commercial/advertising spam offering special incentives for quick and easy weight-loss products and programs and "business opportunities" in classifieds advertisements. Work at home schemes, such as making arts and crafts or stuffing envelopes have been replaced by offers to "use your home PC to make fast money in your spare time." Job-related spam came in third at 10 percent of all spam messages sent. Meanwhile, research by PandaLabs revealed 40 percent of all rogue anti-virus has been created this year. It said since this type of malicious code was first reported 4 years ago, 5,651,786 unique rogueware strains have been detected, out of which 2,285,629 have appeared between January to October 2010. A report said: "If we compare the number of rogueware specimens to the total number of malware strains included in our Collective Intelligence database, 11.6 percent of all samples correspond to fake anti-virus. This is a staggering figure, especially if you consider that this database contains all malware detected in the company's 21-year history and rogueware only appeared 4 years ago." Source: http://www.scmagazineuk.com/almost-half-of-all-rogue-anti-virus-was-created-in-2010-as-uk-based-spam-increases/article/191099/

Symantec claims breakthrough in understanding on how Stuxnet operates and what its targets are. The Stuxnet worm requires the industrial control system to have frequency converter drives from at least one of two specific vendors. According to a Symantec representative, new research that was published late the week of November 8 established that Stuxnet searches for frequency converter drives made by Fararo Paya of Iran, and Vacon of Finland. He said: "The new key findings are that Stuxnet requires particular frequency converter drives from specific vendors, some of which may not be procurable in certain countries. Stuxnet requires the frequency converter drives to be operating at very high speeds. While frequency converter drives are used in many industrial control applications, these speeds are used only in a limited number of applications. Stuxnet also changes the output frequencies and thus the speed of the motors for short intervals over periods of months. Interfering with the speed of the motors sabotages the normal operation of the industrial control process. Symantec's new detection therefore determined that once operation at those frequencies occurs for a period of time, Stuxnet then hijacks the PLC code and begins modifying the behavior of the frequency converter drives. In addition to other parameters, over a period of months, Stuxnet changes the output frequency for short periods of time to 1,410Hz and then to 2Hz and then to 1,064Hz. Modification of the output frequency essentially sabotages the automation system from

operating properly," he said. Source: http://www.scmagazineuk.com/symantec-claims-breakthrough-in-understanding-on-how-stuxnet-operates-and-what-its-targets-are/article/190903/

U.S. sees huge cyber threat in the future. The United States faces a major threat in the future from cyber technologies that will require civil-military coordination to shield networks from attack, the U.S. Defense Secretary said November 16. "I think there is a huge future threat. And there is a considerable current threat," he told The Wall Street Journal CEO Council. The Defense Department (DoD) estimated that more than 100 foreign intelligence organizations have attempted to break into U.S. networks. Every year, hackers also steal enough data from U.S. government agencies, businesses, and universities to fill the U.S. Library of Congress many times over, officials said. The Secretary said the U.S. military had made considerable progress protecting its own sites and was working with private-sector partners "to bring them under that umbrella." But how to allow Pentagon know-how to be applied to protecting domestic infrastructure can be tricky for legal reasons, including fear of violating civil liberties. "The key is the only defense that the United States has against nation-states and other potential threats in the cyber-world is the National Security Agency," he said, referring to the super-secretive DoD arm that shields national security information and networks, and intercepts foreign communications. Last month, the Presidential Administration announced steps to allow greater cooperation between the NSA and DHS. Source: http://www.reuters.com/article/idUSTRE6AF4UX20101116

Hackers, spammers will target Facebook Messages, say experts. Facebook's revamped Messages will be a very attractive target for spammers, scammers, and malware makers, security experts said November 16. Facebook countered, saying that it has implemented new measures to protect users, including third-party anti-spam filtering of inbound e-mail. On November 15, Facebook unveiled its new Messages, which adds e-mail to the ways members can communicate with friends. An all-in-one inbox collects Facebook messages, instant messages, text messages, and e-mail into a single view. The addition of e-mail means that spammers and scammers have yet another way to reach users, said a senior security adviser at antivirus vendor Sophos. The security adviser compared Facebook's history of combating spam with Google's Gmail, and gave the thumbs up to the latter. "In Gmail, it's not impossible to spam, but it's difficult ... Gmail does a pretty damn good job of protecting users." In a reply to questions, a Facebook spokesman said the company has contracted with a third-party vendor to "supplement our spam detection and protection for messages sent from e-mail addresses off of Facebook." Source: http://www.computerworld.com/s/article/9196828/Hackers_spammers_will_target_Facebook_Messages_say_experts

(Utah) **Changing password may help curb computer virus.** A computer virus plaguing inboxes the week of November 15 appears to be affecting Web-based e-mail accounts. The fix might be as simple as changing a password. The virus can be caught through spam that erroneously looks like it is from the user. It is sent to people the user knows. The subject line is blank and the body of the e-mail contains no text, just an e-mail link. It is invasive, bothersome, and mysterious, and believed to be affecting thousands of people in Utah. The e-mail administrator at Internet Service Provider XMission investigated and found a common link in Web-based e-mail accounts such as Hotmail, Yahoo, and Gmail. In most cases that XMission checked, passwords may have been hacked, allowing access to e-mail address books. Changing passwords appears to be an important, yet simple fix. XMission's vice president of operations said some of the problems have been fixed for providers, but not all. "This is

fairly typical to what is happening all the time. Just follow best practices, good passwords, anti-virus software," he said. Experts said it is wise to have a good password in general — a mix of letters and numbers, at least eight characters long, and not found in the dictionary. Source: http://www.ksl.com/?nid=148&sid=13301520

Imperva warns of rise in Stuxnet hacking threats. State-sponsored hacking, man-in-the-browser, and insider attacks are among the key threats facing organizations in 2011, according to research from Imperva. The data security firm released its top security trend predictions November 15, warning that the likely proliferation of Stuxnet-like attacks means that companies must monitor traffic and set security controls across all organizational layers. To reduce the threat from insider attacks, Imperva recommended tightening controls so access to sensitive information is given only on a need-to-know basis, and to eliminate unnecessary privileges. The sophistication of man-in-the-browser attacks will increase, meanwhile, forcing online service providers to invest in better protection such as strong device identification, client profiling, session flow tracking, and site-to-client authentication. Other trends noted by Imperva include the growing use of sophisticated smartphones in the enterprise, which could present challenges to IT departments as they struggle to include the devices in traditional data and application security practices. Finally, Imperva predicted that social networks will finally begin to take seriously threats such as cross-site scripting attacks by boosting application layer security, and rolling out stronger authentication and account control features. Source: http://www.v3.co.uk/v3/news/2273136/imperva-malware-threts-security

World's most advanced rootkit penetrates 64-bit Windows. A notorious rootkit that for years has ravaged 32-bit versions of Windows has begun claiming 64-bit versions of the Microsoft operating system as well. The ability of TDL, aka Alureon, to infect 64-bit versions of Windows 7 is something of a coup for its creators, because Microsoft endowed the OS with enhanced security safeguards that were intended to block such attacks. The rootkit crossed into the 64-bit realm sometime in August 2010, according to security firm Prevx. According to research published November 15 by GFI Software, the latest TDL4 installation penetrates 64-bit versions of Windows by bypassing the OS's kernel mode code signing policy, which is designed to allow drivers to be installed only when they have been digitally signed by a trusted source. The rootkit does this by attaching itself to the master boot record in a hard drive's bowels and changing boot options. Prevx researchers said TDL is the most advanced rootkit ever seen in the wild. It is used as a backdoor to install and update keyloggers and other types of malware. Once installed it is undetectable by most antimalware programs. In keeping with TDL's high degree of sophistication, the rootkit uses low-level instructions to disable debuggers, making it hard for white hat hackers to do reconnaissance. Source: http://www.theregister.co.uk/2010/11/16/tdl_rootkit_does_64_bit_windows/

Is a Facebook security hole helping hackers spread iPhone 4 spam? Is a security weakness on Facebook allowing cybercriminals to post spam messages directly onto users' walls. Overnight November 15 into November 16, a number of users saw posting messages like the following on their Facebook walls: "Apple is giving away 1000 Iphone4s i just got mines =)." Clicking on the link takes one to a Web site that promotes a "make money fast" scheme, attempting to recruit home workers. This latest wave of spam messages indicated they were posted "via Email". That is the facility Facebook supplies to post status updates to a Facebook page remotely, by sending an e-mail to a unique address (every Facebook account has a specific e-mail address for this purpose). One guess is the facility may have been compromised, and scammers have found a way to update users' statuses

of users by sending an e-mail message directly to their walls. Source: http://nakedsecurity.sophos.com/2010/11/16/facebook-security-hole-iphone-spam/

Nearly 200 Chinese government sites hacked daily. Nearly 200 Chinese government Web sites are hacked every day, with 80 percent of these cyber attacks coming from abroad, said the vice director of the State Information Center of Network and Information Security of China Ministry of Public Security, at the Fourth U.S.-China Internet Industry Forum in Beijing November 9. "Eight out of ten computers with Internet access in China have experienced attacks by botnets," he said. A report issued earlier this year by China National Computer Network Emergency Response Technical Team (CNCERT) showed 71 percent of the world's botnets are located in China. Most of them are controlled by foreign hackers. As a nation that currently has 440 million Internet users, "China is the main victim of online criminals," the vice director said. China cooperates with foreign governments to combat online criminals. So far, Chinese police have established bilateral cooperation with 30 countries including the United States, UK, and Germany. "China and the U.S. have the largest number of Internet users and the largest number of Web sites. We have broad cooperation prospects in combating online crimes. I sincerely invite American delegates coming to exchange views with us, putting forward more efficient mechanism to combat trans-border cyber crimes," the vice director said. Source: http://www.china.org.cn/china/2010-11/11/content_21321167.htm

Cyber experts have proof that China has hijacked U.S.-based Internet traffic. For 18 minutes in April 2010, China's state-controlled telecommunications company hijacked 15 percent of the world's Internet traffic, including data from U.S. military, civilian organizations, and those of other U.S. allies. This massive redirection of data has received scant attention in the mainstream media because the mechanics of how the hijacking was carried out and the implications of the incident are difficult for those outside the cybersecurity community to grasp, said a top security expert at McAfee. The Chinese could have carried out eavesdropping on unprotected communications — including e-mails and instant messaging — manipulated data passing through their country or decrypted messages, McAfee's vice president of threat research said. Nobody outside of China can say, at least publicly, what happened to the terrabytes of data after they entered China. The incident may receive more attention when the U.S.-China Economic and Security Review Commission, a congressional committee, releases its annual report on the bilateral relationship November 17. A commission press release said the 2010 report will address "the increasingly sophisticated nature of malicious computer activity associated with China." Source: http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=249

National Monuments and Icons

(Illinois) **Forest Service: Grassy Knob fire soon will be contained.** The Grassy Knob Fire on the Shawnee National Forest in Illinois remains at 409 acres and will be 100 percent contained by 6 p.m. November 10, according to a release from the U.S. Forest Service (USFS). Most of the resources were demobilized that evening. Firefighters will remain on site to patrol and monitor the fire until the next rain event. The cause of the fire is under investigation. A closure order for the fire area has been issued by a forest supervisor that requires the public to stay out of the area due to safety concerns. Fire personnel and emergency vehicles will be in the area and will need unencumbered access to the fire, according to the USFS release. Source:

http://www.dailyregister.com/newsnow/x647560454/Forest-Service-Grassy-Knob-fire-soon-will-be-contained

Postal and Shipping

(New Hampshire) **White powder causes Passport Center evacuation.** A "suspicious white powder" found on a package in the mail room at the National Passport/Visa Center at Pease, New Hampshire, prompted an evacuation November 16. According to the assistant fire chief, firefighters and members of the hazardous materials team were called to the 31 Rochester Ave. facility around 8:30 p.m. after an employee in the mail room reported finding the substance. The assistant fire chief said first responders were quickly able to determine the powder was not a threat after testing the substance. The evacuation was routine and part of procedure whenever anything suspicious in nature is found at a government facility, the assistant fire chief said. Source: http://www.seacoastonline.com/articles/20101117-NEWS-101119794

(Oregon) **Downtown Eugene buildings evacuated after bomb threat.** Police said a man who threatened to blow up a van near the Eugene, Oregon post office has been arrested. The Register-Guard said authorities November 16 evacuated nearby buildings, including the Hilton Eugene, after learning of the threat. Police negotiators talked the man out of the van, which was parked outside the post office on Willamette Street. A bomb team found no explosives. A Eugene police spokeswoman said a 62-year-old male from nearby Corvallis was arrested for investigation of disorderly conduct. The FBI and U.S. Postal Inspection Service are working on the investigation. Source: http://www.koinlocal6.com/news/local/story/Downtown-Eugene-buildings-evacuated-after-bomb/IrYytmKBp0ug0-Rvoh7jhA.cspx

U.S. knew for years that cargo planes were terror targets. Lobbying by the multibillion-dollar freight industry helped kill past efforts to impose tough rules on air cargo. The U.S. government failed to close obvious security gaps amid pressure from shipping companies fearful tighter controls would cost too much and delay deliveries. Intelligence officials around the world narrowly thwarted an Al Qaeda mail bomb plot last month. But it was a tip from Saudi intelligence, not cargo screening, that turned up the bombs before they could take down airplanes. Company employees in Yemen were not required to X-ray the printer cartridges the explosives were hidden inside. Instead, they looked at the printers and sent them off, U.S. officials said. In 2004, when the Transportation Security Administration (TSA) considered requiring screening for all packages on all flights, the Cargo Airline Association downplayed a terrorist threat. It argued slowing down shipping for inspections would jeopardize the shipping industry and the world's economy. The government wanted security, TSA said, "without undue hardship on the affected stakeholders." The U.S. requires all packages be screened before being loaded onto passenger flights originating in the United States. But there is no such requirement enforced for all cargo loaded onto U.S.-bound international passenger flights or on cargo-only flights, such as UPS and FedEx planes. Source: http://www.foxnews.com/us/2010/11/09/knew-cargo-planes-vulnerable-years/

Public Health

(Florida) **Florida woman diagnosed with cholera.** A woman who recently returned to Florida from Haiti has been diagnosed with cholera, the Florida Department of Health (FDH) announced November

17. An outbreak of the disease in Haiti has killed more than 1,100 people there, health officials said. "We have laboratory confirmation that it is the type of cholera spreading in Haiti," an FDH spokesman said. "This is not a major public health concern, but we're on top of it," he added. The woman has been released from the hospital where she was being treated and is doing well, he said. "We are working with our health care partners to ensure appropriate care of this individual and prevent the spread of this disease within the community," the Florida Surgeon General said in a written statement. Florida authorities will "continue to monitor the state for any future cases," she added. The FDH noted that the superior U.S. infrastructure minimizes the risk for fecal contamination of food and water, limiting the potential spread of the disease. Person-to-person transmission is rare, it added. In the past 5 years, 44 cases of cholera have been reported in the United States, according to statistics from the Centers for Disease Control and Prevention. Source: http://www.cnn.com/2010/US/11/17/florida.haiti.cholera/index.html?hpt=T2

(Florida) **Deputies investigate hospital bomb threats.** Law enforcement agencies in three Central Florida counties were investigating bomb threats made at three Florida Hospital locations November 16. Authorities in Lake, Orange, and Osceola counties said calls were received at Florida Hospital Waterman (Tavares), Florida Hospital East, and Florida Hospital Kissimmee, respectively. In Orange County, deputies said an unidentified female caller said there was a bomb on the hospital property, located at 7727 Lake Underhill Road. Hospital personnel decided to shut down the emergency room to incoming patients, but patient care inside the hospital was not interrupted. Investigators believed the call was a hoax; however safety precautions were taken and after two-and-a-half hours, the scene was cleared and it was determined that the threat was unfounded. There were similar calls placed at the two other hospitals. All sites were cleared of any danger. Source: http://www.myfoxorlando.com/dpp/news/orange_news/111610deputies-investigate-hospital-bomb-threat

Laptop thefts top cause of health data breaches. Laptop theft is the most prevalent cause of the breach of health information affecting more than 500 people, according to the Health & Human Services Department (HHS), which last year began tracking data breaches by public and private healthcare organizations. The fact that laptops are so easily stolen underscores the importance of physical security in the protection of health information, according to a senior health IT and privacy specialist in HHS' Office for Civil Rights. Of the 189 records of data breaches affecting more than 500 individuals in the first year, 52 percent were from theft. About 20 percent were from unauthorized access and disclosure of protected information, while 16 percent were from loss, he said November 10 at the mHealth Summit conference. Laptops were involved in 24 percent of data breaches affecting more than 500 people and paper records were close behind at 22 percent. Desktop computers accounted for 16 percent of the breaches and portable devices accounted for 14 percent. His advice is to "encrypt, encrypt, and encrypt. The information remains protected to a significant degree," he said, even when the device falls into the wrong hands. Source: http://www.healthcareitnews.com/news/laptop-thefts-top-cause-health-data-breaches

TRANSPORTATION

Government reports: U.S. could do more to reduce traffic deaths. Two new government reports claim America could do a better job promoting safety on the country's roads. The first, released by the National Research Council, showed recent U.S. declines in traffic fatalities have been outpaced by

other developed nations. The United States could do a better job of road design and traffic management; regulation of vehicle safety; and regulation of driver behaviors regarding speed, alcohol and drug use, and seat belt and motorcycle helmet use. The second report is an update to the National Transportation Safety Board's (NTSB) "most wanted" list of safety improvements. The NTSB added motorcycle safety to its most wanted list, replacing recreational boating. The NTSB's most wanted list is a directive to states where they can best focus safety resources. Among the other items on NTSB's "wish list" are eliminating distractions for young drivers, improving child occupant protections, enacting primary-enforcement safety-belt laws, and cracking down on habitual drunk drivers. Source: http://blogs.consumerreports.org/cars/2010/11/us-could-do-better-at-reducing-traffic-fatalities-say-2-government-reports.html

(New York) **New York subways not prepared for a mass evacuation, bombshell lawsuit claims.** The New York City subway system is ill-prepared for a mass evacuation in the case of a fire, explosion, or terrorist attack, and a judge needs to command the Metropolitan Transportation Authority (MTA) to fix the "very dangerous and potentially lethal" conditions, according to a whistleblower lawsuit filed by a 25-year MTA veteran in Brooklyn federal court November 17. In August 2007, the former superintendent in the division of station operations, told his bosses that the "anti-crime" gates — which make it possible to close off alternate entrances and exits to subway stations during certain times of the day — were open, but not padlocked open. That meant someone could enter the station, close the gates, and lock them, creating "a very dangerous and potentially lethal event in an emergency situation," like an explosion, bomb threat, or chemical or biological attack, the suit said. The former superintendent also claimed the MTA provided him with too few chains and padlocks for the gates, and when transit bosses took a survey of how many were unsecured, "the actual safety conditions in the field were being underreported in the survey." Source: http://www.nypost.com/p/news/local/brooklyn/subways_not_prepared_for_mass_evacuation_UMwjMQHWM5b0PN0BtnIEJP

Airline Wi-Fi sparks security concerns. A new potential safety issue has arisen for airlines: Does Wi-Fi service given to passengers pose any sort of danger aboard a plane? The question arose after Yemeni terrorists tried recently — and failed — to destroy two U.S.-bound cargo planes by stuffing printer cartridges full of explosives and then detonating the charges in flight. According to a explosives consultant, Wi-Fi "gives a bomber lots of options for contacting a device on an aircraft. "We recognize the potential of the threat and are looking at it closely," said the spokesman for the International Federation of Air Line Pilots' Associations (ALPA). "We need to fully explore what could the bad guys do, how could this be turned against us," said a Boeing 737 pilot and chairman of the national security committee for ALPA. Source: http://www.ajc.com/news/nation-world/airline-wi-fi-sparks-743309.html

U.S. officials defend new airport screening procedures. DHS officials defended heightened airport security screening measures November 15, but said they would consider adjustments to new rigorous patdowns after complaints from travelers. With the busy holiday travel season about to begin, the Homeland Security Secretary made it clear that new full-body scan checks would become the routine as hundreds of the machines are installed at U.S. airports and that the alternative would be physical patdowns. "This is all being done as a process to make sure the traveling public is safe," she said, adding that the scans did not pose health risks and that privacy safeguards have been adopted to prevent the images from being saved or transmitted. There are almost 400 body scan machines in

some 68 U.S. airports. Some airports still only use metal detectors. Source: http://www.reuters.com/article/idUSTRE6AB5B820101115

(California) **California's Bay Bridge shut down by man who claims explosives in car: report.** A distraught man who claimed he had explosives in his car and threatened to jump off California's San Francisco - Oakland Bay Bridge was taken into custody November 11, ending an hour-long standoff with police, KTVU-TV said. The man called emergency dispatchers around 7 a.m. and told police he had a pipe bomb in his SUV. He then pulled over his car on the bridge. All westbound morning rush-hour traffic on the bridge was brought to a halt as the San Francisco bomb squad, the California Highway Patrol, and hostage negotiators responded. The man had climbed over the bridge's protective barrier and on to the ledge. He was allegedly threatening to kill himself and blow up the bridge. The man was talked into surrendering and was arrested around 8 a.m. The bridge's upper deck remained partially closed as authorities checked the vehicle for explosives, but the car was eventually cleared and moved off the bridge around 8:30. A man claiming to be the person on the bridge called a local radio station to say he had pulled over on the bridge with his daughter and had explosives and a gun, KTVU-TV said. A female passenger, said to be the man's daughter, fled after the man pulled over and was safe with authorities. Source: http://www.nypost.com/p/news/national/california_report_bridge_shut_down_eCVbcUJdiY4L7ncxNPBtlL

(Texas) **Avoid travel in Amarillo.** The Amarillo, Texas Police Department issued a traffic message November 11 at 10:29 p.m. They warned motorists to avoid travel in Amarillo. Several roads were impassable due to high water levels. The emergency operation center for the City of Amarillo asked drivers to stay off roadways except in emergency situations. Travel along I-40 and I-27 was extremely dangerous and several intersections were impassible. Source: http://www.valleycentral.com/news/story.aspx?id=539738

Water and Dams

(California) **U.S. EPA orders Caltrans to comply with Clean Water Act to protect state waters.** The U. S. Environmental Protection Agency (EPA) has ordered the California Department of Transportation (CalTrans) to upgrade its statewide stormwater management program, and exert stronger controls over stormwater discharges from its road construction and maintenance sites. The Clean Water Act enforcement action follows a series of EPA field audits of four Northern California CalTrans districts. Accompanied by state and regional water board representatives, EPA inspected numerous CalTrans construction and maintenance sites, and found violations of the California-issued stormwater permit designed to protect the state's water resources from polluted stormwater runoff. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/9635D2E39894B2A1852577DD0062CFDE

(California) **Regulators require replacement for contaminated water.** Pacific Gas and Electric (PG&E) must provide clean drinking water to residents in Hinkley, California whose groundwater has abnormally high levels of a cancer-causing pollutant, water regulators announced in a November 16 memo. The Lahontan Regional Water Quality Control Board said it will formally issue the order by November 30, but a PG&E spokesman said the utility company is already distributing water bottles to six residents whose wells have more than 3.1 parts per billion of hexavalent chromium. That is the same limit the board is proposing, because chromium exists naturally in the town's groundwater.

Tests showed plumes of chromium — made famous by then-legal clerk Erin Brockovich's successful lawsuit against PG&E in 1996 — spreading again in March. A water board spokeswoman said the board is considering an additional order regarding wells with levels of the contaminant lower than 3.1 parts per billion, but rising relative to what earlier tests showed. Source: http://www.tradingmarkets.com/news/stock-alert/pcg_regulators-require-replacement-for-contaminated-water-1314012.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**